We are IntechOpen, the world's leading publisher of Open Access books Built by scientists, for scientists

4,800
Open access books available

122,000
International authors and editors

135M
Downloads

Our authors are among the

154
Countries delivered to

TOP 1%
most cited scientists

12.2%
Contributors from top 500 universities

CLARIVATE ANALYTICS BOOK CITATION INDEX INDEXED

WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?
Contact book.department@intechopen.com

Numbers displayed above are based on latest data collected.
For more information visit www.intechopen.com

4

When the Industry Goes Wireless: Drivers, Requirements, Technology and Future Trends

Simon Carlsen[1] and Stig Petersen[2]
[1]*StatoilHydro ASA, Harstad,* [2]*SINTEF ICT, Trondheim*
[1,2]*Norway*

1. Introduction

Through the last ten to fifteen years wireless communication technology has become a natural and fully integrated part of our everyday lives. The two most exposed applications, digital mobile telephony and wireless computer networks, are so common that it is hard to imagine a world without these technologies. In addition, a number of different everyday devices in the home, in the car or in the office communicate with each other over short range wireless links, utilizing technologies like Bluetooth or similar.
Even though what is said above may seem obvious to most people in the industrialized world, the situation is somewhat different when it comes to applications of wireless technology in the industry itself. Compared to the numerous applications of wireless communication that we all are so familiar with and have learned to consider as indispensable from a consumers' point of view, the benefits of wireless solutions in industrial applications have until the last few years not been so obvious. Of course, different industries and companies are at different stages regarding the implementation and adoption of wireless technology, but in general we see a conservative approach, and the reasons for such a progression are many.
This chapter will deal with some important aspects as the industry slowly evolves from a wired world into the wireless domain. It is organized as follows; section 2 examines the motivations and drivers for introducing wireless technology within the industry, section 3 presents the industrial requirements which the wireless technology must fulfil in order to be a viable option to today's wired solutions, section 4 gives an overview of the most relevant international standards for industrial wireless communications, and section 5 concludes the chapter by identifying the current trends and important future research areas for industrial wireless technology.

2. Applications, drivers and motivation

To enable the introduction of any new technology in the enterprise, a major driver and motivational factor is the potential financial gains, i.e. reduced costs and/or increased

revenue. Secondly, if new technology has the potential to benefit other important aspects such as health, safety or the environment (HSE), they would also be considered interesting for the industry. Potential areas in which wireless technology can be beneficial to the industry can be divided into three distinct applications; mobile ICT (information and communication technology), wireless instrumentation, and asset and personnel tracking.

2.1 Mobile ICT

The development and rapid deployment of systems adhering to the IEEE Std 802.11 for wireless local area networks (WLANs) have enabled Internet access to mobile devices such as laptops, personal digital assistants (PDAs) and high-end mobile phones, from nearly anywhere at any time. WLAN access points are deployed in office buildings, public spaces, airports, cafeterias and in private homes, providing either free or purchasable Internet access to everybody in the vicinity. While wireless access in the home, office or public spaces mainly has focused on internet access and access to enterprise systems on the office network, the focus is somewhat different for industrial applications. Some relevant application areas involving the use of mobile ICT in the industry includes:

- Simplification of work processes
- Simplify or automate routine test procedures
- 'Bringing the control room to the field'
- Online field access to status, maintenance logs etc for instruments and components as a part of fault diagnostics procedures
- Inspection and maintenance tasks by means of WLAN enabled mobile cameras, where the field operator communicates in real-time over video and audio with remote expert centres

Commonly, mobile ICT applications in the industry are associated with local on-site WLAN networks, which to date has more or less followed the same implementation strategy as for WLANs' in office environments. The benefits for deploying local network infrastructure are many. For example, it ensures sufficient bandwidth for demanding applications, and the security and data integrity aspects are locally controlled.

In some industries, however, the costs for deploying local infrastructure for enabling wireless coverage in the process areas can be significant. This is particular relevant in industries which comprise explosive atmospheres, such as Oil & Gas and mining. In such areas, very strict restrictions apply regarding requirements for all electrical apparatus intended for use inside specific zones. In Europe, the ATEX directive (European Parliament and the Council, 1994) contains the governing rules, regulations and requirements for the use of electrical equipment in hazardous environments. Other countries have similar directives, for example in North America and Canada the North American Hazardous Locations Installation Codes (National Electric Code for the US and the Canadian Electrical Code for Canada) define rules and regulations on equipment and area classifications requirements for hazardous locations. Network equipment planned for use in such areas must be certified to conform to these regulations. In practise, this involves either regular equipment built into specially designed enclosures, or it demands for complete redesigns of the equipment itself. The certification is a comprehensive process that can only be carried out by selected certification agencies. This leads to significant increases in equipment cost. As an example, a WLAN access point manufactured for corporate use has a cost of approximately 800 – 1,000 USD in its ordinary version. The ATEX-certified version (the

same access point built into an enclosure, and the unit certified as a whole), has a cost in the order of 8,000 – 10,000 USD, e.g. the price has increased by a factor of ten. In addition, strict installation procedures for equipment in process plants are further cost-driving parameters. The above facts, combined with a general lack of pre-certified WLAN equipment in the market designed for use in explosive atmospheres, has been a showstopper for the rapid deployment of large-scale mobile ICT in industries like the Oil & Gas. For these reasons, these industries have started looking at public networks such as GPRS and UMTS as alternative access channels.

We end this section by giving an example on the use of mobile ICT to simplify a work process in the process industry. The example is taken from (Petersen et al., 2008).

2.1.1 Example – Simplifying maintenance routine jobs

Traditionally, work processes in process industries involve a number of manual operations. A typical workflow for operation and maintenance tasks is presented in Fig. 1. The flowchart illustrates how several activities have to be performed in a given order. If we consider a maintenance operation where notifications and work orders are required, typically the whole process has the following (simplified) progression from a field operators' point-of-view:

1. Initiate operation
2. Create a notification. This is commonly done with the corporate Enterprise Resource Planning (ERP) system
3. Await confirmation from ERP system
4. Create work order through ERP
5. Await signed work permit
6. Prepare operation
7. Plan operation
8. Execute maintenance operation
9. Close operation
10. Verify technical condition restored
11. Update documentation, both in technical documentation systems and ERP

Wireless network access in the field can help simplify this process. Consider a Personal Digital Assistant (PDA) with wireless access to the company's backbone systems. The PDA is equipped with an RFID or barcode reader for reading information from tagged plant equipment.

When the field operator detects a faulty component that is subjective to maintenance, the tag of the component is read or scanned with the PDA. A notification describing the upcoming maintenance operation is created on the PDA. This information is then transmitted via the wireless network into the ERP system.

As soon as the necessary confirmation is received, a work order is created. During the maintenance operation, the field operator can update the technical documentation online from his mobile device. As a finishing activity, a verification of the technical condition of the component has to be performed, commonly requiring that the operator is physically present in the field. When the verification is passed, the operator is able to remotely flag the status of the work order as finished using the PDA.

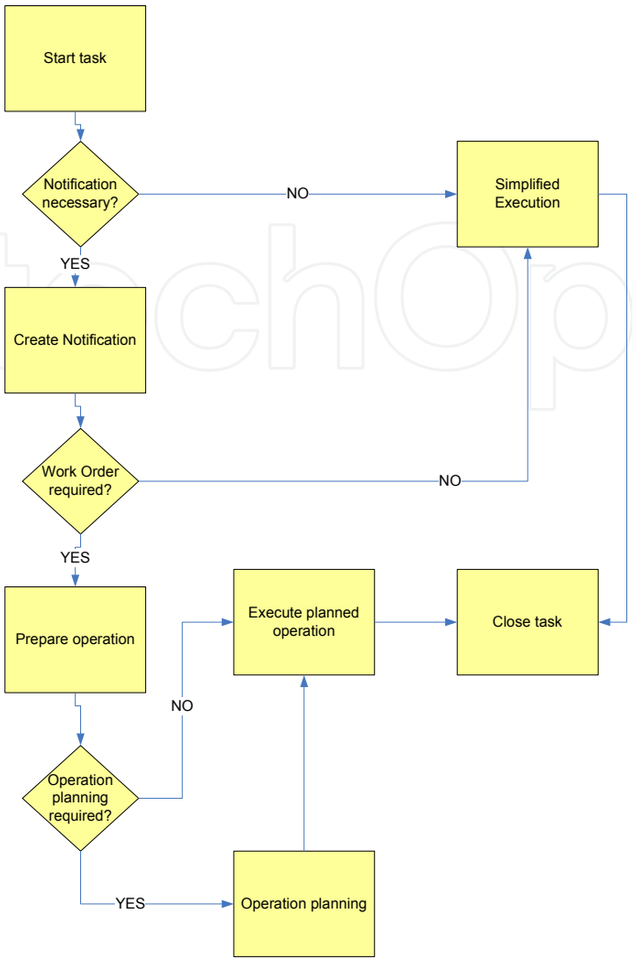

Fig. 1. Typical workflow for mainteance operation

2.2 Wireless instrumentation

Recent advances in wireless technology have enabled the development of low-cost, low power wireless sensors capable of robust and reliable communication (Akyildiz et al., 2002). The IEEE Std 802.15.4 (IEEE 802.15.4, 2006) defines the physical layer (PHY) and the medium access control sublayer (MAC) for low-rate wireless personal area networks. Inherent features such as ultra-low complexity, cost and power makes it a very suitable standard for wireless sensor network (WSN) solutions (Yu, Q et al., 2006). With a growing number of both standardized and proprietary solutions based the IEEE Std 802.15.4 PHY and MAC appearing on the market, it has quickly become the *de facto* standard for WSNs.

Using sensors to monitor both the performance and the operational environment of industrial plants and facilities allows for greater insight into operational requirements and potential safety problems. The sensors are used to monitor a wide range of parameters, e.g. pipeline pressure, flow, temperature, vibration, humidity, gas leaks, fire outbreaks and equipment condition. The collected sensor data is then used to make informed just-in-time decisions on plant performance and operational conditions. It is expected that the

continuing advances in WSN technologies will enable wireless sensing, monitoring and control applications within the following industrial areas (Petersen et al., 2007):

- Condition and performance maintenance monitoring
- Area and property surveillance and monitoring
- Environmental monitoring
- Emergency management
- Process control

In addition, eliminating the need for cables will contribute to reduced installation costs, and extend coverage into areas previously either too remote or too hostile to be viable for wired instrumentation. Furthermore, using wireless sensors provides the possibility of doing temporary installations and mobile installations, for example in conjunction with turnarounds and shutdowns. So, flexibility and installation time are major beneficial factors making the use of wireless sensors very cost-effective compared to traditional instrumentation.

As an example on a real-world application, a wireless sensor network was installed at an oil production platform in the North Sea. The complete scenario is extensively described in (Carlsen et al., 2008)

2.2.1 Example – Using Wireless Sensor Networks to Enable Increased Oil Recovery

The actual oil field is in its tail-end lifecycle, and, combined with the geological structure consisting of many small oil accumulations, occasional loss of flow from the wells was not readily detected, which lead to unplanned stops in the production. During the construction stage back in the 1980's, no flow metering devices were installed inside the flow lines. Calculations performed by staff personnel at the actual license show that unpredicted stops in production due to unexpected loss of well pressure counts for annual financial losses in the order of 40 million USD. Based on these calculations, it is clear that a reliable, easy to install detection system for alerting upcoming pressure losses is very attractive for gaining increased revenue.

The installation and maintenance of a traditional detection system (flow meters inside the pipes) is complex and requires a complete production shutdown, and was not considered an alternative. Another showstopper for introducing wired sensor equipment in a live production environment is the need for cables. As these units need both wired power and a wired communication link, the complexity and cost factors are high.

A simple approach to determine loss of flow in a well is to measure the temperature of the well flow line, some distance downstream of the wellhead. This is based on the principle that loss of flow causes a reduction in surface temperature of the pipe as heat is lost to the surroundings. The typical well fluid temperature is approximately 60^{o}C, thus the temperature measurement can be performed on the pipe's surface. This eliminates the need for an invasive installation, which greatly simplifies installation. Until recently, loss of flow from individual wells was detected by plant operators manually probing the surface temperature of the flow lines during inspection rounds one or two times each 12 hour shift. By introducing battery-operated wireless temperature sensors clamped on to the outer surface of the pipes, the installation of the sensor unit is simpler and wires can be eliminated. The installation is not time-consuming and can be performed during normal operation of the facility.

The bottom line is that the wireless sensor network approach has been very successful. The estimated increased revenue has been achieved, and the wireless network has been close to 100 % reliable with no loss of sensor data through the 1 ½ year period it has been in operation. Integration with the existing PCDA system was implemented utilizing the serial MODBUS interface of the wireless gateway, and real time monitoring with automatic triggering of alarms when the pressure declines is managed from the PCDA. Because of the immediate success of the pilot installation, several other Oil & Gas producing facilities in the North Sea recently have deployed similar wireless sensor networks.

2.3 Asset and personnel tracking

Keeping track of assets and personnel is getting increasingly important as industrial operations are becoming more and more complex. We see a growing number of new products and concepts for local area tracking of assets and people. These are alternative solutions in applications where public services such as GPS (Global Positioning System) or similar is not a viable alternative. It is common to distinguish between Real-Time Localization Systems (RTLS), where the tag position is being updated in real-time and passive tracking utilizing RFID, in which the tag is detected when passing a checkpoint.
Some industrial application areas involving tracking solutions include:

- Keeping track of containers and goods at supply bases
- Keeping track of expensive tools and parts, as lost and misplaced equipment can interrupt production or slow down planned work. It also contributes to reduce duplicate captures of similar assets
- Keeping track of people in emergency situations, for example by RFID-based counting and identification of people at choke points (meeting points or mustering stations)
- Keeping track of goods and assets in the whole logistics chain, from manufacturer to end-user

The following section provides an example of a planned asset tracking system for simplifying the logistics on an onshore supply base, serving offshore Oil & Gas installations in the North Sea. The example is taken from (Petersen et al., 2008).

2.3.1 Example – Improving container logistics

At a supply base, there are a large number of container movements every day, year round. Keeping track of the physical location of each container is considered a challenge, and requires extensive logistics. In addition, it is essential to know the contents of each container. Keeping track of individual container positions along with container metadata is an application where wireless networks can improve efficiency.
Each container is equipped with an electronic tag, serving as a unique ID. Before the container leaves its origin, the tag information is updated. Using a centralized database, the tag ID can be linked with container specific data.
During transportation, the container passes several checkpoints equipped with RFID readers, enabling tracking of the container on its way towards the destination. Events during transport (customs inspection, reloads etc) is logged online and added into the central database. When the container arrives at the supply base, its presence is detected by either an RFID chokepoint or the plant-wide wireless network. A field operator equipped

with a mobile device, e.g. PDA or laptop computer, can access the metadata of the container by making a request to the central database.
As the container is moved around at the base, its physical position can be monitored by utilizing the positioning capabilities of the plant-wide RTLS-enabled WLAN network. Typically, positioning data is linked with a map of the site, visualizing the position of the container in real-time. When container goods is added or removed, the field operator can update the central database using a wireless mobile device.
In order for the concept of container tracking to be successful, tight integration between the wireless network, the positioning application, the database server, user applications, the Enterprise Resource Planning (ERP) system and mobile devices is required.

3. Requirements

A set of requirements have been identified for the use of wireless technology in industrial applications. Some are of a general nature and adhere to all types of wireless equipment, devices and networks. They are:

- Security – Every mobile communication technology should support mechanisms for securing the information flow and ensure data integrity. As a minimum, link layer encryption comprising 128-bit keys should be a general requirement for industrial applications.
- Mechanical Reliability – For industrial applications, the equipment should be industry-grade with respect to mechanical quality and robustness (IP-rating etc.)
- Certification for Operation in Explosive Areas – In some industries many areas are defined as explosive zones. All equipment for use in these areas must be certified according to the national regulations. In the EU, the law is the ATEX directive.
- International standards – Technologies for wireless communication should be comprised by international standards. This ensures interoperability between equipment from different vendors.
- ISM (industrial, scientific and medical)-bands – To ensure global, license free operation, wireless systems should wherever possible use the international ISM frequency bands for the radio communication.
- Coexistence – Friendly coexistence with other systems operating in the same portions of the frequency spectrum. That is, not cause interference to other systems, and be resilient to interference from other systems.
- User Interface - the user interfaces for wireless systems must be able to provide a simple and intuitive interface for advanced configuration, control and management.
- Cost-effective – Wireless systems must be cost-effective, both in terms of installation and daily operation, compared with wired alternatives.

In addition to these general requirements, a set of specific requirements for each of the identified main application areas for industrial wireless technologies have been worked out.

3.1 Mobile ICT

As mobile ICT involves the widest spans of applications within wireless communication, the requirements naturally become very application dependent. Anyway it is still possible to

identify some requirements related to mobile ICT in industrial settings are of a general nature. These include:

- Security and Authentication – Among the most important issues in IEEE 802.11 networks. As the wireless network commonly represents an extension of the corporate network providing access to backhaul systems, the highest levels of security and authentication mechanisms should be implemented. Security should be employed at both link and network layers (Layer 2 and 3 in the OSI model, respectively), and should preferably be centrally managed. Features such as rotating encryption keys and exchange of certificates through dedicated servers (RADIUS or similar) should be a requirement. For all mobile devices that provide logon and user authentication features, this should be enabled using identities and passwords that can be tracked back to the individual user
- Bandwidth – Industrial WLAN applications commonly require less bandwidth than corporate or consumer market applications (but higher reliability). Medium bandwidth is a general requirement, but this is of course application dependent
- Reliability – IEEE 802.11 networks inherently do not provide the necessary level of reliability to make them suitable for any application of critical nature. A medium to high level of reliability, up to 99 %, is a reasonable requirement for the industry. Reliability can be increased by the use of redundant networks or mesh topologies
- Scalability – Easily scalable as the demands for wireless coverage and/or the number of users increases
- Seamless integration – The backhaul network should be fully transparent to the mobile client. Virtually no difference between a wired and a wireless client from a users' point of view
- Site management – To avoid local configuration and administration of huge numbers of infrastructure components in the wireless network, centralized management, configuration and monitoring of the network should be a requirement
- Simplified and automated work processes – Depending on the application, the introduction of a mobile ICT solution in the industry could have as a requirement that a specific work process should be simplified, for example a routine maintenance task being reduced by a given number of man hours. Another application could set up as a requirement that the new mobile ICT solution should fully automate the former manual task

3.2 Wireless Instrumentation

For wireless instrumentation, and in particular wireless sensor networks, the following requirements have been identified (Petersen et al., 2007)

- Reliability – For general monitoring applications, reliability should be > 99.99 %, e.g. maximum acceptable data loss is 1 sample out of 10,000 samples. Note that even a network with a significant packet loss can achieve 100 % reliability due to retransmissions and redundant paths
- Battery lifetime – For battery operated wireless sensors with a one minute update rate, the battery lifetime should be in excess of 5 years

- Update Rate – Requirements for necessary sensor data update rate should be stated. For IEEE 802.15.4 networks, update rates down to 1 minute is practically achievable. Note the trade-offs between update rate and power consumption
- Simple maintenance routines – Wireless instruments should be designed and installed in such a manner that routine maintenance, e.g. exchange of batteries, can be easily performed
- Transparency to wired systems – From an end-users' (operator) point of view, there should be virtually no difference between a wired instrument and its wireless counterpart
- Integration to control room – Wireless instruments should integrate with existing control and monitoring systems over standard industrial interfaces (field buses etc)
- Security and authentication – The networks should be resilient to both active and passive security threats and attacks (Cayirci & Rong, 2009).

3.3 Asset and personnel tracking

As is the case for mobile ICT, the requirements for asset and personnel tracking depends on the specific usage scenario. The following general requirements should be applicable to most industrial asset and personnel tracking applications:

- Precision – Precise requirements on position resolution and accuracy should be worked out, as this contributes to the premises for which localization technology that should be chosen
- Real-Time – Depending on the application, real-time requirements regarding update of position should be stated
- Infrastructure demands – Asset and personnel tracking solutions can either utilize public infrastructure, existing enterprise infrastructure, or deploy new infrastructure depending on the application and the technology
- Redundancy – Depending on the level of criticality of the application, requirements for fail-safe operation and redundant solutions should be carried out. Keywords are redundant networks, alternative networks and uninterruptible power supplies
- Client side or network side positioning – Depending on the application, the calculations for determining the mobile devices' position should either be carried out on the device itself (which requires computational power), or on a central server located at the backhaul side of the network
- Maintenance free tags – Locatable tags must have a lifetime in the order of several years in order to be maintenance free and cost effective

4. Wireless Technology and International Standards

This chapter provides a survey of the most relevant technologies and international standards for industrial wireless communication. For some applications, solutions from the consumer and office markets are adapted by the industry. However, in many cases this technology, or the equipment itself, does not fulfil the industrial requirements. Modifications, or even redesigns, are therefore often needed in order to enable industrial deployment. The growing demand for industry specific applications of wireless technology

within mobile ICT, wireless instrumentation and asset and personnel tracking has lead to the development of specific technology and international standards for industrial use:

- **Mobile ICT**
  IEEE Std 802.11
- **Wireless Instrumentation**
  IEEE Std 802.15.4, ZigBee, WirelessHART and ISA100.11a
- **Asset and personnel tracking**
  Various RFID standards and the ISO 24730 for Real-Time Localization Systems

4.1 IEEE Std 802.11

The 802.11 working group of the IEEE standards body is responsible for defining and maintaining a set of standards for Wireless Local Area Networks (WLAN). The original (legacy) IEEE Std 802.11-1997 defined three Physical (PHY) Layer specifications and one common Medium Access Control (MAC) specification. Since then further work has been carried out to extend the initial PHY specifications to provide higher data rates, leading to IEEE Std 802.11a and IEEE Std 802.11b, both released in 1999, and IEEE Std 802.11g, released in 2003. In 2007, all the addendums to the legacy IEEE Std 802.11-1997 was merged and published as IEEE Std 802.11-2007 (IEEE 802.11, 2007). The new revision collects many of the changes and amendments performed and published by IEEE 802.11 Task Groups. In addition, the IEEE Std 802.11n (IEEE 802.11n, 2009) was published in 2009.
Table 1 provides an overview of the different 802.11 protocols.

Protocol	Release Date	Frequency (GHz)	Data Rate (Mbps*)
802.11	1997	2.4	2
802.11a	1999	5	54
802.11b	1999	2.4	11
802.11g	2003	2.4	54
802.11n	2009	2.4 and/or 5	600

** Megabit per second*

Table 1. Overview of the IEEE Std 802.11 protocols

4.1.1 IEEE 802.11 Operation Modes

The IEEE Std 802.11 defines two pieces of equipment, a wireless station/client and an Access Point (AP), which acts as a bridge between the wireless stations and wired networks. The AP acts as the base station for the wireless network, aggregating access for multiple wireless stations onto the wired network.
There are two operation modes in IEEE 802.11, infrastructure mode and ad-hoc mode**.** In infrastructure mode the wireless network consists of at least one AP connected to a wired network infrastructure, and a set of wireless stations. This configuration is called a Basic Service Set (BSS). An Extended Service Set (ESS) is a set of two or more BSSs forming a single sub-network. Ad-hoc mode is a set of wireless stations that communicate directly with one another without using an AP or any connection to a wired network.

4.1.2 The legacy IEEE Std 802.11-1997

The original IEEE Std 802.11-1997 defines operation in the 2.4 GHz band, supporting data rates of 1 and 2 Mbps. The IEEE Std 802.11 divides the 2.4 GHz band into 14 channels, each with a bandwidth of 22 MHz. However, due to national rules and regulations, channel 14 is only available in a select few countries (Japan, Spain), and channels 12 and 13 are prohibited in North American and some Central and South American countries. The centre frequency of the channels are spaced 5 MHz apart, which means that neighbouring channels overlap in frequency.

IEEE Std 802.11-1997 uses Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). CSMA/CA is referred to as the Distributed Co-ordination Function (DCF). This requires each station to listen for other users. If the channel is idle, the station may transmit. However if it is busy, each station must wait until transmission stops at which time the receiver sends an ACK. Then each station must wait for a time equal to the Distributed Inter-Frame Space (DIFS), plus a random number of slot times for the next transmission in order to avoid collisions over the medium.

4.1.3 IEEE Std 802.11a

The IEEE Std 802.11a (IEEE Std 802.11, 2007) operates in the 5 GHz band, using the same core protocol as the other IEEE 802.11 specifications The 5 GHz band offers the advantage of avoiding the popular and crowded 2.4 GHz band, but the higher frequency reduces the communication range, and makes it more sensitive to interference from walls or other architectural components. This necessitates the use of more access points to achieve comparable coverage to its 2.4 GHz counterparts. IEEE Std 802.11a uses a 52-subcarrier Orthogonal Frequency-Division Multiplexing (OFDM) modulation scheme with a maximum raw data rate of 54 Mbps.

Although IEEE Std 802.11a offers increased bandwidth capacity over IEEE Std 802.11b, it is not widely adopted. It has become difficult to acquire IEEE Std 802.11a AP or PC cards as IEEE Std 802.11b/g have developed as the *de facto* standard for both the consumer and industrial markets.

4.1.4 IEEE Std 802.11b

The IEEE Std 802.11b (IEEE Std 802.11, 2007) is an amendment to the original IEEE 802.11-1997 standard. It supports data rates of 5.5 and 11 Mbps in the 2.4 GHz band by using Complementary Code Keying (CCK) with Quadrature Phase Shift Keying (QPSK) modulation and Direct-Sequence Spread-Spectrum (DSSS) technology.

The IEEE Std 802.11b defines dynamic rate shifting, allowing data rates to be automatically adjusted for noisy conditions. This means that IEEE Std 802.11b devices will transmit at lower data rates (5.5 Mbps, 2 Mbps or 1 Mps) under noisy conditions. When the devices move back within the range of a higher-speed transmission, the connection will automatically speed up again.

4.1.5 IEEE Std 802.11g

The IEEE Std 802.11g (IEEE Std 802.11, 2007) is another amendment to the IEEE Std 802.11-1997. It further extends the maximum raw data rate in the 2.4 GHz band to 54 Mbps. IEEE Std 802.11g hardware is backwards compatible with IEEE Std 802.11b, but the presence of an

IEEE Std 802.11b client in a IEEE Std 802.11g network will significantly reduce the overall data rate of the IEEE Std 802.11g network.
The IEEE Std 802.11g adds a new section to the IEEE Std 802.11 PHY; the Extended Rate PHY Specification (ERP). The ERP adds the data rates of 6, 9, 12, 18, 24, 36, 48 and 54 Mbps to the rates already defined by IEEE Std 802.11-1997 and IEEE Std 802.11b. Of these rates, support for 1, 2, 5.5, 11, 6, 12 and 24 Mbps is mandatory.
Two additional optional ERP-PBCC modulation modes with data rates of 22 and 33 Mbps are also defined. In addition, another optional modulation mode, DSSS-OFDM (Direct Sequence Spread Spectrum-Orthogonal Frequency Division Multiplexing) with data rates of 6, 9, 12, 18, 24, 36, 48 and 54 Mbps is defined.
An ERP device is capable of operating in any combination of available modulations.

4.1.6 IEEE Std 802.11n

The IEEE Std 802.11n (IEEE Std 802.11n, 2009), ratified in 2009, supports operation in both the 2.4 and 5 GHz bands simoultaneously. It is backwards compatible with all three previous IEEE Std 802.11a/b/g protocols. IEEE Std 802.11n opens for a theoretical maximum raw data rate of 600 Mbps. One of the major additions to the IEEE Std 802.11n PHY is the added capability of using 40 MHz channel bandwidth (Perahia & Stacey, 2008). This channel bonding merges two adjacent 20 MHz channels into one single channel. The adjacent channel interference is equal for 20 MHz and 40 MHz operation. As the 2.4 GHz band only has three available non-overlapping channels (channel 1, 6 and 11), this means that IEEE Std 802.11n equipment may occupy 2/3 of the available spectrum.
To handle coexistence and interoperability issues arising when using a 40 MHz channel, the two 20 MHz channels used to form the 40 MHz channel are defined as primary and secondary channels. Control and management (beacons) are transmitted on the primary 20 MHz channel, and legacy 20 MHz devices (IEEE 802.11a/b/g) will use the primary channel for all communication. In addition, the legacy portion of the 20 MHz mixed format preamble is replicated over both 20 MHz channels. Even though 40 MHz channel bandwidth is possible (and allowed) in the 2.4 GHz band, it is not recommended duo to potential coexistence issues with other network and devices operating in the 2.4 GHz band.
IEEE Std 802.11n will also make some improvements to the IEEE Std 802.11 OFDM mechanisms. A short guard interval has been introduced, reducing the guard interval of the OFDM data symbols from 0.8 μs to 0.4 μs. The overall symbol length is reduced from 4 μs to 3.6 μs. The guard interval of the preamble is not modified to ensure compatibility with legacy devices. The short guard interval corresponds to an increased data rate of 11 % compared to legacy devices. An option to make the preamble more efficient is also included in the IEEE Std 802.11n, using a Greenfield preamble. The Greenfield preamble reduces the overhead of the PHY preamble by 12 μs compared to the legacy mixed format preamble. The Greenfield preamble is however not compatible with legacy devices.
Several modifications to the IEEE Std 802.11 MAC layer are done in order to increase the throughput of an IEEE Std 802.11n network. Results from the IEEE 802.11e task group work on Quality of Service enhancements to the IEEE 802.11 family have been added. This includes data burst - where several data packets from a single source are transmitted continuously without pausing between each packet – and immediate block acknowledgement. Other new MAC mechanisms for the IEEE Std 802.11n is reduced inter-frame space (RIFS), where the space/time between two following frames are reduced. For

one-way data intensive applications (i.e. file upload or download), it is also an option to completely remove the inter-frame spacing through data aggregation.
Several additions to the IEEE 802.11n standard make the data exchange more robust than for the legacy standards. The receive diversity enabled by MIMO allows for maximal-ratio combining (MRC), and the possibility of transmitting different bits over separate antennas. With MIMO there is also the possibility of having more antennas than spatial streams. Improved error detection and correction codes are also introduced in IEEE 802.11n, both space-time block coding, and the optional low density parity check (LDPC) codes.

4.2 IEEE Std 802.15.4

The IEEE Std 802.15.4 defines the physical (PHY) and medium access control (MAC) layers for low-rate wireless personal area networks (IEEE 802.15.4, 2006). The standard specifies operation both in the 868/915 MHz band and in the 2.4 GHz band. Two new, optional high-data-rate PHYs in the 868/915 MHz band were introduced in the 2006 revision of the standard.
The IEEE Std 802.15.4 defines a total of 27 channels, numbered 0 to 26. Channel 0 is in the 868 MHz band with a centre frequency of 868.3 MHz. Channels 1 through 10 are located in the 915 MHz band. The channel spacing is 2 MHz, with channel 1 having a centre frequency of 906 MHz. Channels 11 through 26 are located in the 2.4 GHz band. The channel spacing is 5 MHz, with the centre frequency of channel 11 being 2.405 GHz.

4.3 ZigBee

The ZigBee specification (ZigBee Alliance, 2006) defines network and application layers on top of the IEEE Std 802.15.4 PHY and MAC, enabling a low-rate, low power WSN. ZigBee is primarily targeting home automation and consumer electronics applications (Verdone et al., 2008). As a ZigBee network operates on the same static channel (one of the 16 available channels defined by IEEE Std 802.15.4) throughout its entire lifetime, it is susceptible to noise and interference. This has lead to ZigBee not being regarded as robust enough for industrial environments and applications. To combat this, the ZigBee Alliance has created the ZigBee PRO specification (ZigBee PRO, 2007) which is specifically aimed at the industrial market. ZigBee PRO offers both enhanced security features and the ability for a network to change its operating channel when faced with large amounts of noise and/or interference.

4.4 WirelessHART

The HART Field Communication Specification, Revision 7.0 (HART 2007) which was ratified in September 2007, has presented the industry with the first open standard, often referred to as WirelessHART, specifically targeting wireless instrumentation for factory automation. WirelessHART is based on the IEEE Std 802.15.4 PHY, although WirelessHART only defines operation in the 2.4 GHz band.
WirelessHART employs a frequency hopping, multi-hop, mesh network topology, using time-division multiple access (TDMA) for channel access. The network communication is divided into time slots, and each communication link in the network is given its own, reserved time slot in order to ensure contention free utilization of the radio channel. This requires all nodes in the network to be time-synchronized, normally using the gateway as

the master clock. With its self-healing and self-configuration capabilities, the deployment of a WirelessHART network does not require detailed understanding of low level communication and radio propagation aspects (Kim et al., 2008).

4.5 ISA100.11a

The ISA100 standards committee of the International Society of Automation (ISA) is working on a family of standards defining wireless systems for industrial automation and control applications (ISA100 Standards Committee, 2008The first released standard was the ISA100.11a (ISA100.11a, 2009), ratified in September 2009, providing secure and reliable wireless communication for noncritical monitoring and control applications. Critical applications are planned to be addressed in later releases of the standard.
The ISA100.11a is based on the IEEE Std 802.15.4 PHY and MAC. It operates in the 2.4 GHz band, and defines a frequency hopping, multi-hop mesh network. Like WirelessHART, TDMA is used as the channel access method, along with network self-configuring and self-healing algorithms. The ISA100.11a enables a network to carry existing wired fieldbus protocols, allowing existing wired installations to be conveniently converted to a wireless infrastructure, with a transparent data transfer between systems.
The ISA100 has also established a subcommittee to investigate options for the convergence of WirelessHART and ISA100.11a, the ISA100.12. The aim of this committee is to merge the two standards into a single standard which will be merged into a future release of the ISA100.11a.

4.6 RFID – Radio Frequency Identification

The term Radio Frequency Identification (RFID) is used for describing identification technologies where a *reader* identifies one or several *transponders* by using electromagnetic waves. The technology has its conceptual origins from IFF (Identify Friend or Foe) systems used to identify aircraft during World War II.
There are no formal definitions of the concept "RFID – Radio Frequency Identification". However, the following description should cover most aspects of RFID technologies:

> **Radio Frequency Identification - RFID**
> Identification performed by the use of electromagnetic waves. The identification process involves at least one *reader* and one *transponder*, and the process is initiated by the reader generating an electromagnetic signal. Compatible transponders within reach of this signal will make a response, enabling them to be detected and identified by the reader.

According to this description, a transponder should only respond after being interrogated by a reader, indicating that transponders should be completely silent (or "invisible") when not interrogated. This restriction is convenient when it comes to distinguishing traditional RFID technology from other identification solutions based on for instance WLAN and Bluetooth. Note however that some proprietary technologies may be described as RFID solutions without conforming to this principle.

4.6.1 Variants of RFID technology

There are several types of RFID technologies on the market. Depending on how they work and how they are constructed, they can be placed in different categories. The two main distinctions are whether the transponders have internal battery or not, and whether the technology is based on *inductive* or *electric* communication (Finkenzeller, 2003).

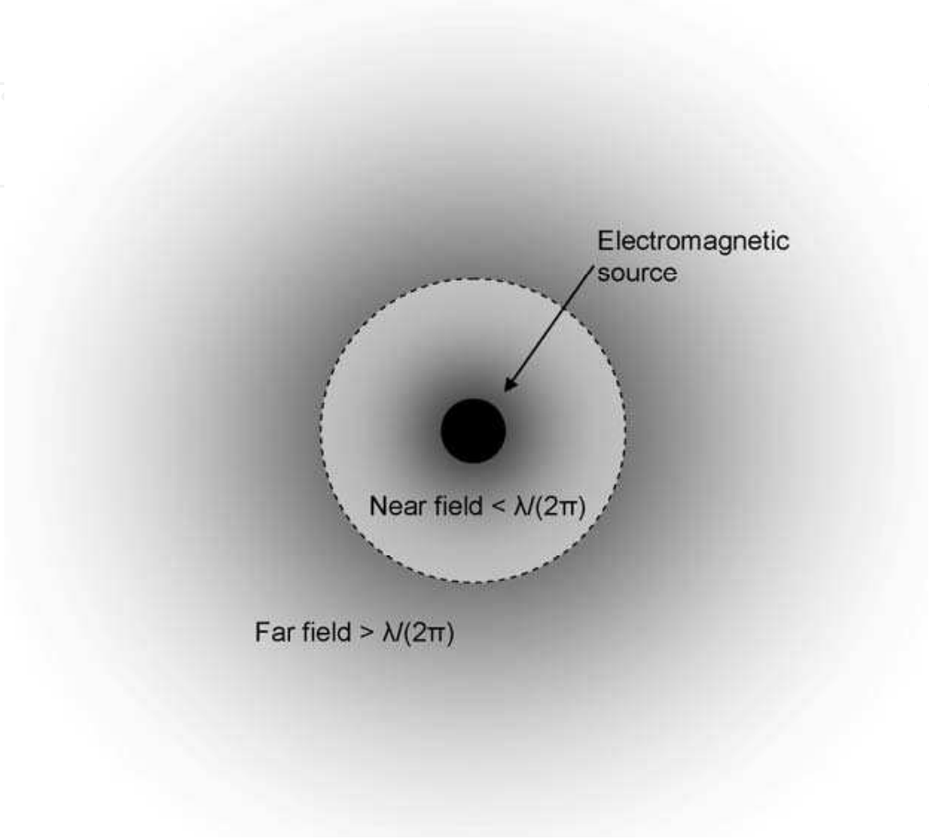

Fig. 2. Illustration of near field and far field (wavelength is denoted by λ)

Active vs. passive transponders

All RFID transponders need energy in order to operate, and many transponder types harvest energy from the reader's electromagnetic field in order to function. Such transponders are called *passive*, as they can only operate when energized by an external energy source. *Active* transponders on the other hand, use an internal energy source (battery) to yield a response. Both technologies have their advantages; while passive RFID transponders, in theory, have no life-time limitations, active transponders can provide much longer read ranges due to their internal power source. A semi-active (sometimes called semi-passive) transponder is a mixture of both active and passive transponders. These do contain a battery, but this battery is only used for internal purposes and not for communication (in which case the transponders would have been classified as active).

Inductive vs. electric communication

RFID technology is either based on *inductive (*magnetic*)* or *electric (*radio-based*) communication*, depending on their operating frequencies (Finkenzeller, 2003). This is due to

the nature of electromagnetic waves, which are created by the magnetic field enclosing the antenna. When a transponder is within a reader's near field (defined as the volume enclosed by a ball with a radius equalling 0.16 times the wavelength of the electromagnetic field), the electromagnetic field has not yet completely formed, and the most efficient way to communicate is by using a coil. Conversely, when a transponder is within a transmitter's far field (that is, outside the near field), the magnetic field is no longer present, and one has to use the electromagnetic field to communicate (as illustrated in Fig. 2). For far field communication, antennas are the most efficient way of receiving and transmitting electromagnetic waves. Note however that the term *antenna* in practice is used for both coils (used for inductive coupling) and "traditional" antennas that are used for electromagnetic communication.

4.6.2 RFID Standards

There are several RFID solutions on the market, of which some are proprietary while others are based on open standards. The most commonly used standards are listed in Table 2.

Frequency	Technology	Standards	Range	Applications
125-135 kHz	Inductive coupling	ISO 11784	< 50 cm	Animal identification
		ISO 11785		
		ISO 14223		
13.56 MHz	Inductive coupling	ISO 14443	< 10 cm	Ticketing, identification and payment
		ISO 15693	< 1 m	
860-960 MHz	Radio backscatter	ISO 18000-6	< 2m	Electronic Product Code

Table 2. Overview of RFID standards

4.7 Real-Time Location Tracking Systems

This section gives a brief introduction to the technology forming the basis for various Real-Time Location Tracking Systems (RTLS). There exist a number of different technologies for determining the position of a device in real-time. As wireless technology increasingly enters the industry, we see a fast growing number of applications utilizing different methods for localization of assets or personnel. In 2006, the International Organization for Standardization, ISO, released the ISO 24730 describing RTLS systems in information technology. The ISO 24730 classifies RTLS into the following:

- Locating an asset via satellite. Accuracy to 10 m
- Locating an asset in a controlled area, e.g. warehouse or similar. Accuracy down to 3 m. Requires local infrastructure
- Locating an asset in a more confined area. Accuracy down to centimetres. Requires local infrastructure
- Locating an asset over a terrestrial area utilizing cell-phone base stations or similar. Accuracy 200 m

In addition, for RFID, two additional methods for locating an object are defined:

- Locating an asset by detecting if it has passed a checkpoint A but not passed checkpoint B

- Locating an asset by the aid of a homing beacon in such manner that a person with a mobile device can find the asset

Observe that the two latter methods are not true RTLS.
In the following section, we give an overview of some of the most widely used technologies for positioning. Each technology has its benefits and disadvantages, depending on the application.

4.7.1 Cell of Origin

In cellular communication systems, e.g. GSM, one simple method to locate a client is by monitoring which base station (cell) the client is associated with. In the case the client is within coverage of several cells, determinate which cell that detects the highest RF signal strength from the client. The cell of origin technique is inaccurate and in general provides a very coarse indication on the clients' position. The position of the client falls within the coverage area of the particular cell. Depending on the cell density and network topology, this area can be large, thus leading to poor determination of position. However, cell of origin is widely used in e.g. emergency call services and is valuable in many applications. If we draw parallels to WLAN networks, the cell of origin principle could be termed as "nearest access point detection".

4.7.2 Received Signal Strength (RSS)

Measuring a clients' RSS at the base station gives an indication of the distance between the two, by the use of lateration techniques. Parameters that must be taken into account are transmitting power, cable losses and antenna gain, and eventually antenna directivity.
Using a suitable mathematical model, the *path loss* between mobile device and access point can be calculated. A common model for indoor propagation at 2.4 GHz is (Cisco Systems, 2008):

$$PL = PL_{ref} + 10 \cdot \log(D^n) + S \quad [\text{dB}] \tag{1}$$

where

PL	is the total path loss between access point and client	[dB]
PL_{ref}	is the reference path loss at a distance equal to 1 m	[dB]
D	is the distance between access point and client	[m]
N	is the path loss exponent, specific to the environment	
S	is the contribution from *shadow fading*	[dB]

Path loss represents the difference between transmitted and received power, and can be seen upon as the signal attenuation throughout the environment. Common factors contributing to signal attenuation are:

- Free space propagation attenuation, equals –6dB per doubling of distance
- Reflections from ground and surroundings
- Diffraction (wave bending effects)
- Scattering (fractional spreading)

The path loss exponent is an empirical parameter specific to the local environment. Typical values for n lie in the range ~2 for open space environments, to >2 in environments with obstructions (Cisco Systems, 2008).
Shadow fading is also related to the environment. The degree of indoor fading varies depending on the number of obstacles present. In a relatively obstructive indoor environment, with many partitions, walls etc, S may be in the range ±7 dB (Cisco Systems, 2008).
The received signal strength P_{RX} is:

$$P_{RX} = P_{TX} - Loss_{TX} + G_{TX} - PL + G_{RX} - Loss_{RX} \quad [\text{dB}] \tag{2}$$

where (all units in dB)

P_{TX}	is the transmitted power
$Loss_{TX}$	is the total loss factors at the transmitter
G_{TX}	is the antenna gain at the transmitter
P_L	is the path loss from eqn. (1)
G_{RX}	is the receiver antenna gain
$Loss_{RX}$	is the total loss factors as seen from the receiver

To calculate the distance D between client (WLAN tag) and receiver, eqn. (2) can be substituted:

$$D = \sqrt{\log^{-1}\left(\frac{P_{RX} - P_{TX} + Loss_{TX} - G_{TX} + PL_{ref} - S + Loss_{RX} - G_{RX}}{-10}\right)} \quad [\text{m}] \tag{3}$$

In a Wi-Fi infrastructure, the base station is the WLAN access point. With one access point, eqn. (3) represents a circle with radius D. The client is assumed to be somewhere on the circumference on this circle. With three or more access points, *tri-lateration* or *multi-lateration* techniques (similar to the methods used for ToA, see section 0) can be utilized to determine the position of the client.
In principle, both clients and access points can measure signal strength. Because of variations in hardware quality and implementation methods among the different WLAN client vendors, the reported signal strengths on the client-side may not be consistent and thus not very reliable. In addition, RSSI detection functionality demands for additional hardware and computational power compared to what's found on a simple WLAN tag.
Leaving the RSSI measurements to the backhaul side of the network is a more robust solution. Most WLAN sites use backhaul equipment (access points etc.) from the same vendor, which yields identical RSSI measurement metrics. A great number of commercial WLAN tracking systems use network side measurements.
RSSI based location utilizes existing WLAN infrastructure, having the advantage that no specialized network infrastructure need to be deployed. From this point of view an RSSI based localization system is attractive with respect to installation cost and complexity.

At the same time, there are several drawbacks with RSSI localization, regarding localization accuracy. Non-ideal RF propagation properties due to anisotropic conditions in the environment is one of the main factors contributing to degraded accuracy. Thus the theoretical path loss model can deviate significantly from the real-world situation. Typical parameters obstructing the path loss model are multipath propagation, radio interference and attenuation (screening from obstacles).

4.7.3 RF Pattern Matching

Pattern matching further refines the RSSI approach for localization. RF pattern matching relies on comparing an objects' current signal strength pattern against a pre-established location database of signal strength patterns collected in the calibration phase. The calibration process (often referred to as the *training* phase) is commonly a time-consuming task involving measuring signal strengths in a large number of pre-determined positions throughout a grid enclosing the coverage area. Once calibrated, the location accuracy within the area can be good in the order of down to a couple of meters. However, as time passes the physical environment is likely to change (equipment, machinery or inventory moves around, climatic conditions change etc) and the accuracy slowly degrades. To accuracy, periodic re-calibration is necessary.

4.7.4 Time-Based Location Tracking Techniques

The common aim for time-based location tracking techniques is, as the name indicates, to give a measure of the distance between the client and one or more base stations utilizing time measures. Two common methods are built on the Time of Arrival (ToA) and the Time Difference of Arrival (TDoA) principles. In this text, the theory behind these positioning principles is taken from (Forssell, B., 1991) and (Cisco Systems, 2008).

4.7.5 Time of Arrival (ToA)

For line-of-sight situations, in particular outdoor environments, the Time of Arrival principle is one of the most accurate methods for determining the position of a receiver. Satellite positioning systems such as the Global Positioning System, GPS (US), Glonass (Russia) and the upcoming Galileo system (EU) use ToA for determining the distance between the base station and the client. For these systems the base station is a space satellite and the client is a mobile receiving unit on the Earths surface.

In ToA, synchronized clocks in the base station and the client are used to measure the time delay between the two. The base station transmits a signal containing information about the exact moment of time t_1 when the transmission occurred. On the client side, this time instant is subtracted from the actual time t_2 and yields a time difference $\Delta t = t_1 - t_1$

Knowing the propagation speed of radio waves c (which is close to the speed of light), the distance r between base station and client can be calculated from

$$r = c \cdot \Delta t = c \cdot \left(t_2 - t_1 \right) \tag{4}$$

Assuming that the exact position of the base station is known, by receiving signals from three (or more) transmitters, the client position can be calculated by performing *triangulation* or *multi-lateration* operations.

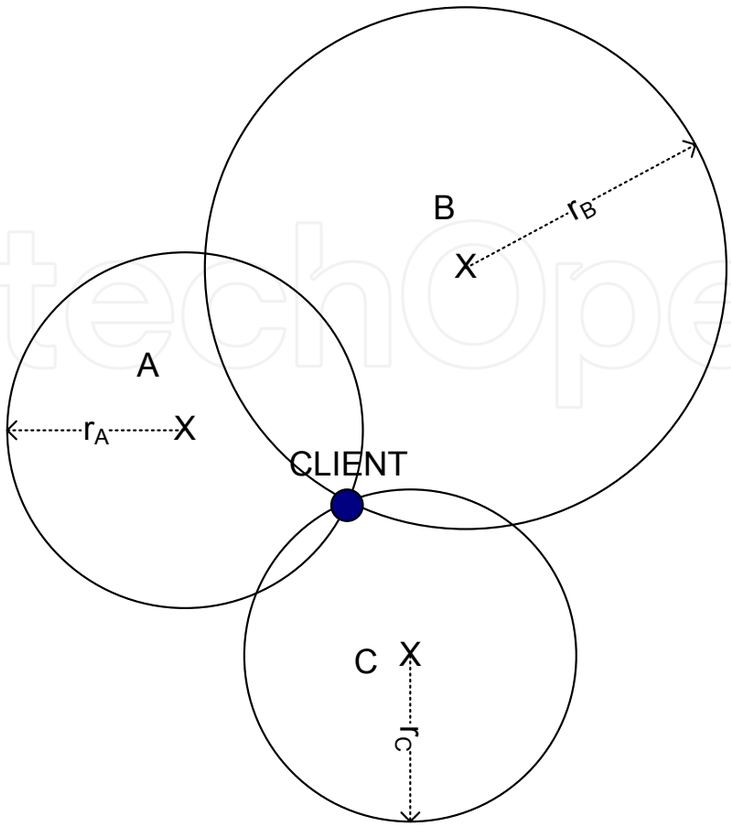

Fig. 3. Triangulation (Tri-lateration)

Using eq. (4), the distance from each base station can be calculated. For every base station - client distance r_n, it is assumed that the position of the client is somewhere along the circle with radius r_n. Signals from three base stations lead to a point of intersection of the three circles, which represents the actual 2D-position of the client. This is illustrated in Fig. 3. For 3D positioning, the client must be within range of at least four base stations. In this case, the intersection point of four constructed spheres represents the 3D-position of the client.

A ToA based positioning system need very accurate and synchronized clocks. To achieve a sufficient level of accuracy, satellite navigation systems use atomic clocks. The client must be time-synchronized with the space satellite. The precision of the time-synchronization is of critical importance to the system performance, as a time measurement error on the scale of a few hundred nanoseconds might cause localization errors in the order of tens of meters.

Furthermore, all calculations for determining the actual position are performed on the receiver side of the network, which demands for sufficient computational power on the client. Additionally, the propagation of radio waves through the atmosphere is exposed to varying delays. This means that the speed of propagation, c, is not constant. For short-range communication this may not be a problem, but in satellite based navigation systems the distance from base station to receiver is in the order 19,000 km to 23,000 km (system dependent), thus varying propagation speeds through the Earths atmosphere will indeed affect the accuracy. Another interfering factor is multipath transmission. The performance of a ToA system is degraded in situations where the received signal is a reflection of the

original signal. Military versions of GPS (and Glonass) transmit on a second frequency to correct for the abovementioned inaccuracies, but receivers are not available for the civilian market. Instead, to increase the localization accuracy for high-precision civilian GPS applications, terrestrial reference stations are used. This technique is referred to as *Differential GPS*, or DGPS.
Achieving true ToA in for example a WLAN network is a challenging task that is difficult to implement with current technology, especially on the client side.

4.7.6 Time Difference of Arrival (TDoA)

When ToA requires synchronized clocks of both base stations and clients, the Time Difference of Arrival (TDoA) approach does not require time synchronization on the client side. Only clock synchronization between base stations is necessary. This is advantageous in the sense that keeping the receiver accurately synchronized with the base stations requires very high precision electronics circuits at the receiver side, leading to expensive client equipment. Also, the commonly high power consumption of ToA-based receiving devices makes them less suitable for battery operation.
In TDoA *relative* time differences between several base stations are calculated. The client transmits a signal which is received by the base stations. No timestamp is sent along, thus the starting time of the transmission is unknown. The signal is picked up by the base stations within range. The relative time differences between the different base stations are then calculated. This technique greatly reduces the complexity of the receiver, as the calculations to determine the clients' position is truly performed at the backhaul side of the network. At least three location receivers are required to perform a 2D location of a client. The mathematical method used to implement TDoA is commonly known as *hyperbolic lateration*. An example of a TDoA based global navigation system is the Long Range Aid to Navigation (LORAN) system. The current generation is the LORAN-C, which serves mainly as a global maritime navigation system with base stations forming different 'chains' around the earth. Although still in service, its use is rapidly declining with GPS as the primary replacement.
Utilizing TDoA for WLAN tracking requires specially designed access points (sometimes referred to as *Location Receivers*). The WLAN client will be the transmitting device, for example WLAN tags transmitting beacons which are picked up by the location receivers. Considering the case with two location receivers *A* and *B*, the time difference of arrival between *A* and *B* is calculated from the following:

$$TDoA_{(B-A)} = \left| T_B - T_A \right| = k \tag{5}$$

The calculated value of $TDoA_{(B\text{-}A)}$ can be used to construct a hyperbola with foci at both location receivers *A* and *B*. The tag position is considered to be somewhere along the constructed hyperbola, at a distance *k(c)* meters from the two foci points. All possible locations of the mobile device can thus be represented by:

$$\left| D_{XB} - D_{XA} \right| = k(c) \tag{6}$$

The actual position is represented by a point along the hyperbola. With only two location receivers, no further determination of the exact position can be calculated. Adding a third Location receiver *C*, a second hyperbola can be constructed, e.g. between *A* and *C*.

$$TDoA_{(C-A)} = \left| T_C - T_A \right| = k_1 \tag{7}$$

Again, the position of the mobile device now can be assumed to be somewhere along this second hyperbola, at a distance $k_1(c)$ meters from the foci points of *A* and *C*. Thus:

$$\left| D_{XC} - D_{XA} \right| = k_1(c) \tag{8}$$

The actual position of the mobile device (WLAN tag) can be represented by the intersection point of the two hyperbolas, as illustrated in Fig. 4.

Like ToA, there might be situations where there exists more than one possible solution for the mobile devices' position. In such cases, a fourth base station is needed in order to perform TDoA *hyperbolic multi-lateration*.

TDoA perform best in outdoor environments with little multipath propagation. Also, semi-outdoor environments such as stadiums, logistics sites etc can often achieve good localization accuracy using TDoA. For indoor environments, TDoA is best suited in buildings that are relatively large and open-spaced. In narrow, crowded indoor areas TDoA suffers from reflection and scattering issues. Increasing the bandwidth of the TDoA signal helps improve the performance. The 2.4 GHz implementation commonly used in the WLAN version of TDoA, is described in ISO 24730. The coding used is BPSK/DSSS (Binary Phase Shift Keying/Direct Sequence Spread Spectrum) with a designated bandwidth of 60 MHz. This allows for improved performance in environments with multipath propagation.

Following the TDoA approach for localization in WLAN networks requires the introduction of specialized network infrastructure alongside with the existing access points. Some vendors provide units that have integrated both WLAN access point and location receiver into the same physical enclosure. Upcoming products feature both TDoA tracking functionality and ordinary IEEE 802.11 WLAN access integrated onto the same electronic circuits.

Table 3 summarizes the different tracking technologies introduced in this section.

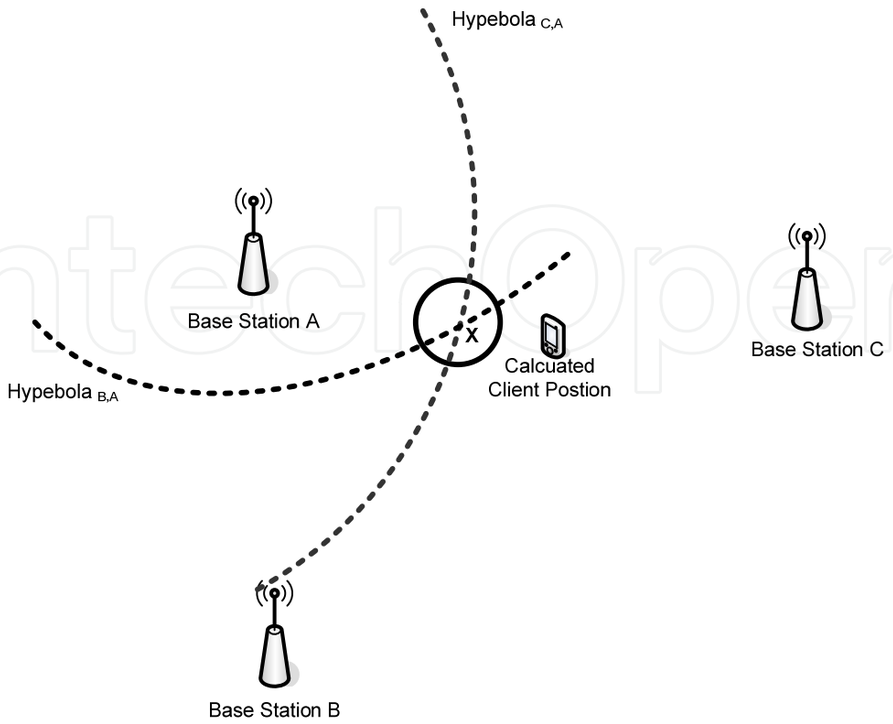

Fig. 4.Time Difference of Arrival (TDoA) with three base stations A, B and C.

Principle	Typical System	Resolution	Line of Sight	Infrastructure cost
Cell of Origin	Cellular communication (GSM, WLAN, etc)	Poor	No	Very low
Received Signal Strength	WLAN networks	Medium	No	Low
RF Pattern Match	WLAN networks with add-ons	Medium to Good	No	Medium
Time of Arrival	GPS or similar	Very good	Yes	Low, but expensive clients
Time Difference of Arrival	Maritime nav. systems, enhanced WLAN networks	Good to Very good	Yes	High

Table 3. Overview of some radio based technologies for real-time localization

5. Future Trends

The basic technologies for wireless communication are already established and proven robust enough for a number of industrial applications, and the number of wireless applications is growing exponentially. But the fact that different wireless suppliers until recently have come up with different devices for different applications, often employing

proprietary radio technologies and communication protocols, have lead to a significant increase in options and complexity for end users. Key questions have emerged in the end users mind about the feasibility of using these devices. This has lead to a growing effort on the standardization of technologies, and this work is still in progress as some aspects of the technology are still are not mature enough for industrial deployment.

For wireless technology development in general, different radio technologies with respect to encoding, channel modulation and protocols, each optimized for the respective application area, is likely to be the case also in the coming years. Related to the OSI Reference Model, it is assumed that the two lowest layers (the physical layer and the data link layer) still need to be service-specific also in the near future. The above layers, however (again referring to the OSI reference model), should be subject to standardization of different wireless technologies. The approach for a common middleware ensures total integration and full flexibility among different wireless technologies individually tailored for different services.

Within the field of wireless instrumentation, several standards have already been established: IEEE 802.15.4, ZigBee, WirelessHART and the ISA100.11a. Currently, these standards are targeting non-critical monitoring and control applications, as there still exists challenges related to the core technology when it comes to wireless process control. As the properties of the wireless medium is of a more stochastic and dynamic nature with respect to interference, transfer delay and service availability compared to wired field buses, issues around reliability and real-time requirements still need to be solved for wireless technology to be a viable option for process control. The IEEE Std 802.15.4 for wireless sensor networks is probably not sufficient for process control applications in its present form. For example, in IEEE 802.15.4 high data reliability is achieved through dynamic routing paths, leading to unpredictable transfer delays. One approach to provide the required quality of service level for wireless process control is to develop a new set of middleware on top of existing base technologies (Chen, D et al., 2004). Others are looking into the development wireless versions of established (wired) industrial communication field buses. More effort needs to be put into the research on wireless process control, with close collaboration between the academia and the industry.

For mobile ICT applications, the IEEE 802.11 family of standards have become the *de facto* standards for wireless networking. For this technology, the future trends will be in the direction of higher bandwidth, extended range, heightened security and increased reliability and robustness in challenging environments. Some of these improvements will be present in the upcoming IEEE 802.11n, which is scheduled for ratification in 2010.

Within mobile ICT and wireless technology for non-critical applications, there still exist some challenges related to the development of intelligent usage areas. More effort should therefore be put into the research on such topics, among them:

- Simplifying work processes
- Automation of routine work operations
- Man-Machine interfaces
- Seamless integration and accessibility to backhaul systems
- Applications to improve Health, Safety and Environmental aspects
- Condition monitoring and maintenance
- Production optimization
- Operational forecasting and prediction
- From decision support to true remote operations

To achieve this, uniform semantics and ontologies across the industry need to be worked out. The time for internal concepts and solutions specific to each organization has definitely passed as a result of globalization in an increasingly complex world. Future requirements for the use of wireless technology in industrial applications will be in the direction of open, standardized solutions which allow full flexibility and compatibly across companies, industries and geography, while at the same time avoiding dependencies to specific vendors. An initiative to standardize the technology and semantics for RFID in the Oil & Gas industry has been initiated by The Norwegian Oil Industry Association (OLF). The project is lead by OLF and the Norwegian research organization SINTEF, with participants from all major license holders on the Norwegian continental shelf. The goal of the project is to investigate Oil & Gas specific requirements for RFID-solutions, and to create a guideline covering aspects such as technology, data capture, communication and system integration within different business applications relevant to the Oil & Gas Industry. Similar initiatives for other technologies and applications will be a necessity to achieve the vision that, in the coming years, wireless technology will be a major and fully integrated part of what is increasingly referred to as "Digital Ecosystems" (DES). A digital ecosystem is a distributed, adaptive, open socio-technical system with properties of self-organization, self-healing, scalability and sustainability, inspired by natural ecosystems (Boley, H. & Chang, E.,2007).

6. References

Akyildiz, I.F.; Su, W.; Sankarasubramaniam, Y. & Cayirci, E. (2002). A Survey on sensor networks, *IEEE Communications Magazine*, Vol. 40, No. 8, pp. 102-114, ISSN 0163-6804.

Boley, H. & Chang, E. (2007). Digital Ecosystems: Principles and Semantics, Proceedings of the Inaugural IEEE-IES Digital Ecosystems and Technologies Conference, pp. 398-403, ISBN 1-4244-0470-3, Cairns, Australia, Feb. 2007.

Carlsen, S.; Petersen, S.; Skavhaug, A. & Doyle, P. (2008). Using Wireless Sensor Networks to Enable Increased Oil Recovery, *Proceedings of the IEEE International Conference on Emerging Technologies and Factory Automation*, pp. 1039-1048, ISBN 978-1-4244-1505-2, Hamburg, Germany, Sept. 2008.

Cayirci, E. & Rong, C. (2009). *Security in Wreless Ad Hoc and Sensor Networks*, John Wiley and Sons, ISBN 978-0-470-02748-6, Chippenham, Wiltshire, Great Britain.

Chen, D; Nixon, M.; Aneweer, T.; Shepard, R. & Mok, A. (2004). Middleware for Wireless Process Control Systems, *Architectures for Cooperative Embedded Real-Time Systems Workshop*, 2004.

Cisco Systems, (2008). *Wi-Fi Location Based Services 4.1 Design Guide*, Text Part Number: OL-11612-01, Cisco Systems.

European Parliament and the Council, "Directive 94/9/EC", 1994.

Finkenzeller, K. (2003). *RFID Handbook 2nd Edition*, John Wiley and Sons, ISBN 0-470-84402-7, Chippenham, Wiltshire, Great Britain.

Forssell, B. (1991). *Radionavigation Systems*, Prentice Hall Europe, ISBN 978-0-1375-1058-0, Oslo, Norway.

HART Field Communication Protocol Specifications, Revision 7.0, 2007, HART Communication Foundation, Austin, Texas.

IEEE 802.11-2007, IEEE Standard for Information Technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 2007, IEEE Computer Society, Washington, DC.

IEEE 802.11n, IEEE Draft Standard for Information Technology – Telecommunications and information exchange between systems – Local and Metropolitan Area Networks – Specific Washington, DC.

IEEE 802.15.4-2006, IEEE Standard for Information Technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs), 2006, IEEE Computer Society, Washington, DC.

ISA 100.11a – 2009, Wireless Systems for Industrial Automation: Process Control and related Applications, 2009, ISA 100 Standards Committee, USA

ISA100 Standards Committee (2008). *The ISA100 Standards – Overview and Status*. Presented at the ISA EXPO 2008, Houston, Texas, USA.

Kim, A. N.; Hekland, F.; Petersen, S. & Doyle, P. (2008). When HART Goes Wireless: Understanding and Implementing the WirelessHART Standard, *Proceedings of the IEEE Conference on Emerging Technologies and Factory Automation 2008*, pp. 899-907, ISBN 978-1-4244-1505-2, Hamburg, Germany, Sept. 2008.

Perahia, E. & Stacey, R. (2008). *Next Generation Wireless LANs*. Cambridge University Press, ISBN 978-0-521-88584-3, Cambridge, United Kingdom.

Petersen, S.; Doyle, P., Aasland, C. S.; Vatland, S.; Andersen, T. M. & Sjong, D. (2007). Requirements, Drivers and Analysis of Wireless Sensor Networks for the Oil & Gas Industry. *Proceedings of the IEEE International Conference on Emerging Technologies and Factory Automation*, pp. 219-226, ISBN 978-1-4244-0825-2, Patras, Greece, Sept. 2007.

Petersen, S.; Carlsen, S. & Skavhaug, A. (2008). Layered Software Challenge of Wireless Technology in the Oil & Gas Industry, *Proceedings of the 19th IEEE Australian Conference on Software Engineering*, pp. 37-46, ISBN 978-0-7695-3100-7, Perth, Australia, March 2008.

Verdone, R.; Dardari, D.; Mazzini, G. & Conti, A. (2008). *Wireless Sensor and Actuator Networks*, Elsevier Academic Press, ISBN 978-0-12-372539-4, Great Britain.

Yu, Q.; Xing, J. & Zhou, Y. (2006). Performance Research of the IEEE 802.15.4 Protocol in Wireless Sensor Networks, *Proceedings of the 2nd IEEE/ASE International Conference on Mechatronic and Embedded Systems and Applications*, pp. 1-4, ISBN 0-7803-9721-5, Beijing, China, Aug. 2006.

ZigBee-2006 Specification, 2006, ZigBee Alliance, San Ramon, California.

ZigBee PRO Specification, 2007, ZigBee Alliance, San Ramon, California.

Factory Automation

Edited by Javier Silvestre-Blanes

ISBN 978-953-307-024-7
Hard cover, 602 pages
Publisher InTech
Published online 01, March, 2010
Published in print edition March, 2010

Factory automation has evolved significantly in the last few decades, and is today a complex, interdisciplinary, scientific area. In this book a selection of papers on topics related to factory automation is presented, covering a broad spectrum, so that the reader may become familiar with the various fields, and also study them in more depth where required. Within various chapters in this book, special attention is given to distributed applications and their use of networks, since it is one of the most relevant subjects in the evolution of factory automation. Different Medium Access Control and networks are analyzed, while Ethernet and Wireless networks are looked at in more detail, since they are among the hottest topics in recent research. Another important subject is everything concerning the increase in the complexity of factory automation, and the need for flexibility and interoperability. Finally the use of multi-agent systems, advanced control, formal methods, or the application in this field of RFID, are additional examples of the ideas and disciplines that experts around the world have analyzed in their work.

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

IntechOpen